Stannp.com

The Communications Platform

Application Security Guide

Overview

Application development is a key Stannp asset, and our applications hold and process highly confidential customer information. Security is a primary function in all our software development and maintenance processes. All software is developed in-house with no third-party development, maintaining complete control over security standards.

Secure Development Practices

Source Code Control - All code changes are versioned using industry-standard tools (Git and GitHub), ensuring all modifications are tracked, auditable, and can be reverted if necessary.

Industry-Recognized Standards - Our developers follow OWASP Top 10 security guidelines with input validation and secure error handling, emphasizing architectural best practices, mandatory testing and coverage requirements, maintainable code, comprehensive documentation, and consistent naming conventions.

Peer Code Review - All code changes are organized into pull requests and reviewed by peer developers before deployment, focusing on security, adherence to standards, and code quality to ensure only secure, well-understood code reaches production.

Environment & Customer Segregation

Separate Environments - We maintain separate development, staging, and production environments to ensure thorough testing before any code reaches live systems, preventing untested code from affecting customer data or service delivery.

Customer Data Segregation - We maintain unique account IDs for each customer, data isolation through multi-tenancy architecture, network-based tenant separation, and regional separation capabilities, ensuring complete data segregation between customers.

Testing & Vulnerability Management

Comprehensive Testing - Applications undergo rigorous automated unit testing with Cypress and integration testing using approved continuous integration tools. Only well-tested code that passes all tests is deployed to production.

Regular Security Testing - Monthly penetration tests and vulnerability scans using Qualys, GitHub automated vulnerability scanning, Azure Cloud Defender, and Security Scorecard for public-facing services.

Risk-Based Patching - Vulnerabilities are scored using CVSS from low to critical risk. Application patches applied within 14-28 days, infrastructure updates within 30 days, with critical vulnerabilities patched immediately (maximum 30 days).

Web Application & API Protection

Advanced Firewall Security - Public-facing applications protected by restricted internet access (HTTP/HTTPS only), automatic blocking of common hacking techniques, and blacklisted IP range filtering.

API Security - Comprehensive protection including authentication tokens, rate limiting, encrypted connections via HTTPS/TLS, detailed access logging, and monitoring for suspicious activity.

Change Management

Formal Change Process - All platform changes follow formal change management with stakeholder approval and documentation. Updates are tested in separate environments before production deployment with unit testing on all upgrades. We communicate significant platform updates that may affect service delivery to clients, ensuring transparency.

Commitment to Security

Our application security policy ensures customer data is protected through comprehensive development practices, rigorous testing, regular security assessments, and immediate response to identified vulnerabilities. With all development performed in-house, we maintain complete control over security standards and quality.